The Hidden Cost of Consumer Data

The more you have, the more you have to lose

whoami

- Christie Dudley
- BSEE, digital communications
- Many years as a network engineer
- 3rd year Santa Clara University Law student
- Consultant assisting with privacy audits

Standard Disclaimer

IANAL (yet)

Walking through a breach

- Barclays business unit in the UK
  - The laws are different there, but analyzing for US
- Significant issues arise due to data volume
- This example illustrates the problem of ever-increasing data collections

Data Stolen

- Complete financial planning dossiers
  - Full contact information
  - Complete list of assets
  - Health information
  - Family status
  - Risk aversion information
- ~27,000 complete records stolen
- Closed business unit

Discovering the Breach

- Confidential informant
- Internal security never knew
- No tracking on how the breach happened

How the Data was Used

- Sold on the "gray market"
- Sold for £50 per record. (~$83)
- Bought by high pressure securities dealers

Liability for the Breach

- Current data breach liability:
  - State law
  - Maybe something from the FTC
- New/old theory of liability:
  - Privacy tort

Some Privacy Tort History

- Warren and Brandeis published "A Right to Privacy" in 1890
- Much litigation and many interpretations at the state level
- Restatement of Torts 2nd identifies 4 common privacy torts in the early 1960's
  - No significant claims since 1977

Recognized Privacy Torts

- Intrusion into seclusion
- Public disclosure of private facts
- Public disclosure that creates a false light
- Appropriation of name or likeness

How are privacy torts new?

- Briefly, "No harm, no foul" in tort-land
- Courts are reluctant to find harm in exposure
- "Loss of enjoyment of life" and other nebulous, but recognized claims don't include privacy.
- Courts look for a specific, articulable harm

Harm from Barclays breach

- High pressure sales to make investments
- Investments made likely to be bad
- Bad investors are traditionally litigious
- Harm here is likely to be significant and specific
- Could result in significant class action
- Damages could extend beyond financial loss

Intrusion Upon Seclusion

- Must invade private affairs of plaintiff
  - Dossiers had full details of the clients' lives, and they were used
- It must be offensive to a reasonable person
  - High pressure sales by people who really know your business
- The intrusion must involve a private matter
  - Financial matters are still considered private
- Intrusion must have caused mental anguish and suffering
  - See above about high pressure sales

Suing Thieves or Barclays?

- Intentional act required for privacy tort claims
- Torts can transfer actor to actor, tort to tort
- If negligence got the ball rolling, it is enough

Negligence

- Data breach is not on its face negligence
- Duty: "Reasonable care"
  - Argued back and forth by lawyers
  - Likely gauged by industry standards
  - Ignorance of breach hurts defense
- DAMAGES
  - Previously not a problem because no damages

Mitigation: Destroy unused data

- Unused data costs money to store, manage and protect
- They can't steal what you don't have

- May need to keep around for regulatory compliance
- Good customer service wants complete data

Mitigation: Keep data offline

- Alternative to destroying
- Far easier to protect: Hard to steal offline data
- Customer service is still not happy

Mitigation: improve data management

- Track where data is stored,
- Limit how customer data is used
- Secure all customer data, not just PII
- Have good logs with meaningful alerts
- Take “reasonable care” in securing and handling all customer data

Conclusions

- Resist collecting and storing everything
- The less available customer data is, the better
- As data grows, so does liability
  - Lawyers can be as crafty as hackers
- Do not lag industry best practices

Thank You

Christie@hackcounsel.com